

**Finding Name: Cross Origin Resource Sharing (CORS) misconfiguration on the web server**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Byeongnam Choe | PT | Project Co-lead | EchoNet |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

I have found a Cross-Origin Resource Sharing (CORS) misconfiguration on the web server. CORS is a browser mechanism that enables controlled access to resources located outside of a given domain. “EnchoNet” uses a wildcard (\*) in the Access-Control-Allow-Origin header, which could potentially cause cybersecurity risks such as cross-domain attacks.

**Risk Rating**  
Impact: Significant  
Likelihood: unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

The wildcard (\*) in the Access-Control-Allow-Origin header allows any domain to access the application's resources, which can lead to attackers performing unauthorized actions or extracting sensitive data. Unauthorized domains might exploit this vulnerability to access or exfiltrate sensitive information. This could damage the company's reputation if the data is compromised, resulting in a loss of trust and confidence from customers.

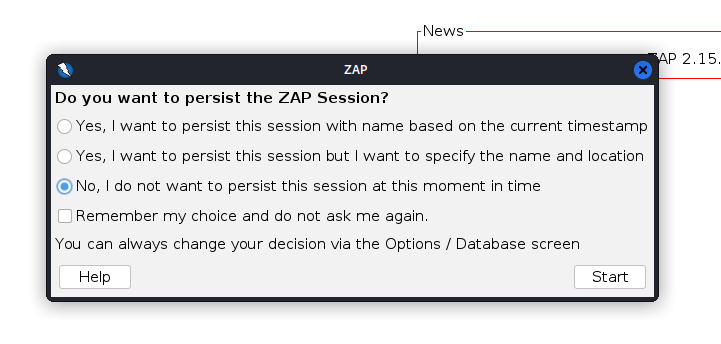
**Affected Assets**

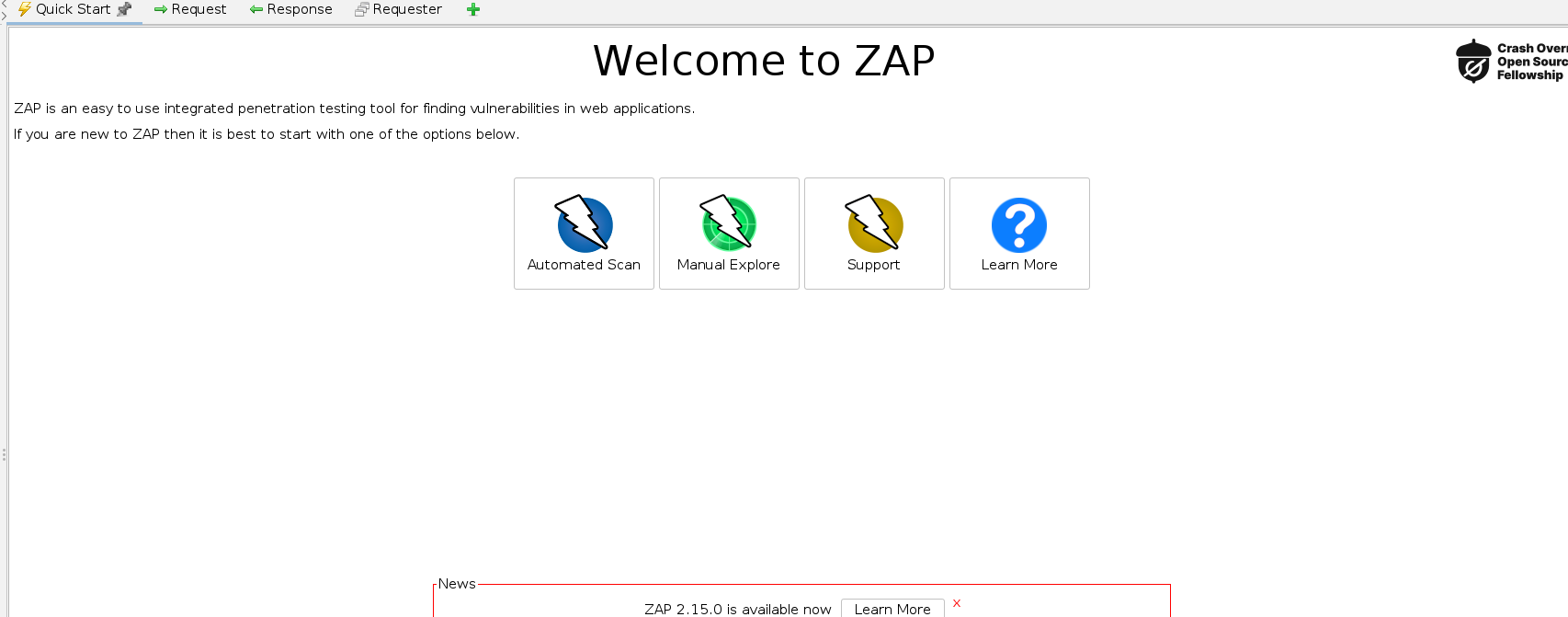
Data

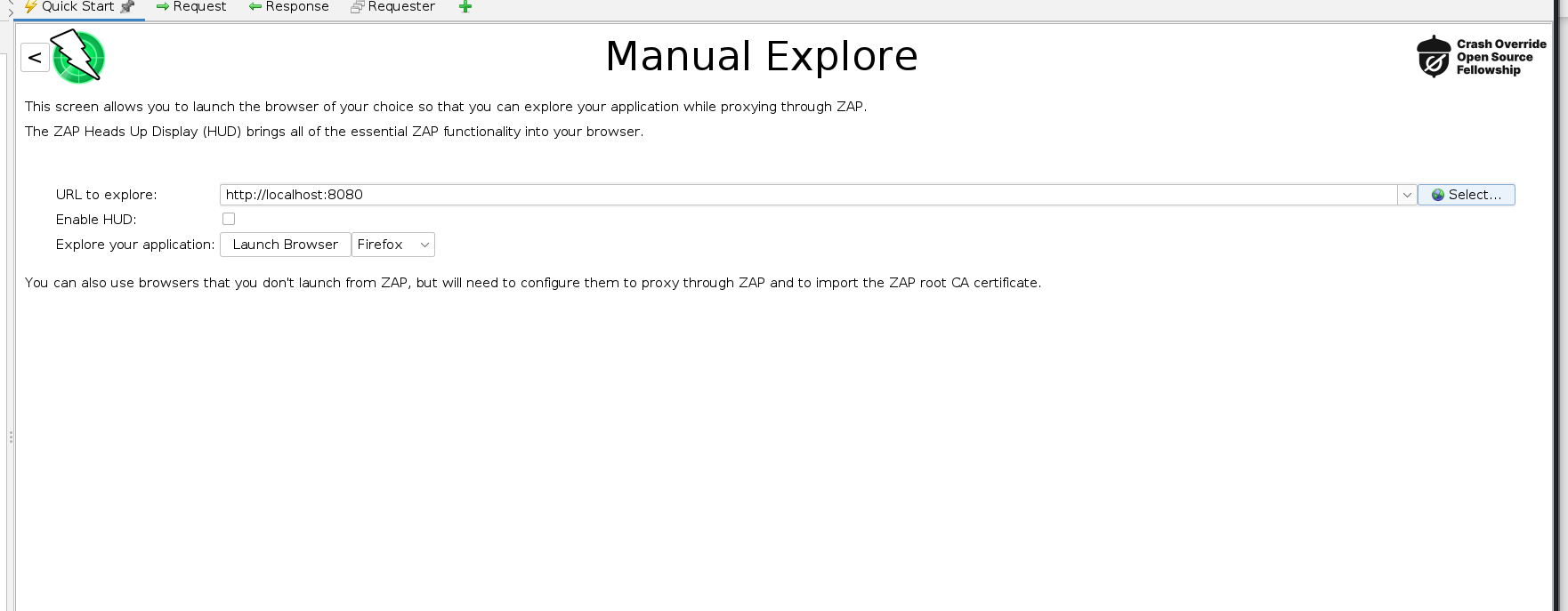
**Evidence**

Provide a step by step guide on how to reproduce the vulnerability with screenshots

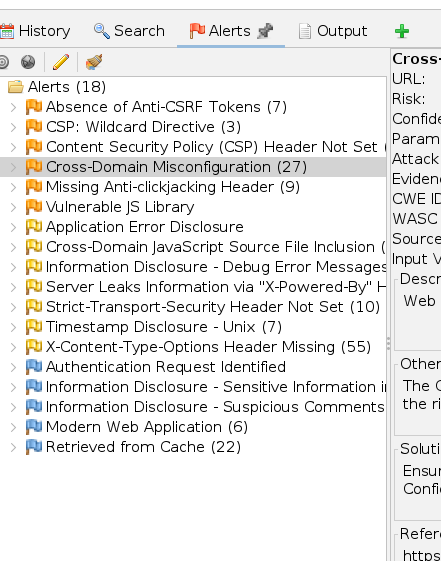
Step 1. Open ZAP to scan the application

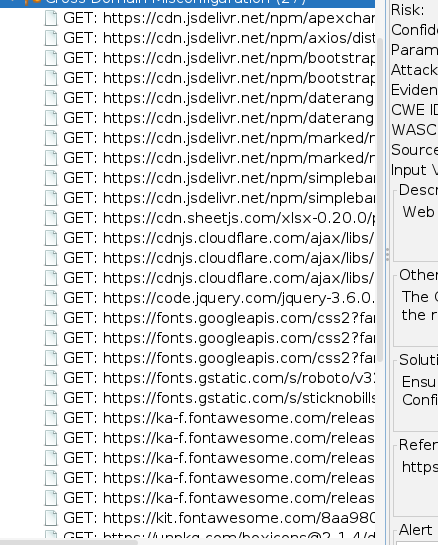
click “No, I do not want to persist this session at this moment in time” to start

Click ”Manual Explore”

 In the section ”URL to explore” enter ”localhost:8080” then click ”Launch browser”

Step 2. discover the misconfiguration in the headers







I found 27 misconfigurations in the headers, as shown in the screenshots above.

**Remediation Advice**

Remove the wildcard (\*) in the header and ensure it points to the trusted domain.

**References**

<https://www.freecodecamp.org/news/exploiting-cors-guide-to-pentesting/>

https://portswigger.net/web-security/cors#what-is-cors-cross-origin-resource-sharing

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on